DEPARTMENT OF THE NAVY
SPACE AND NAVAL WARFARE SYSTEMS COMMAND
4301 PACIFIC HIGHWAY
SAN DIEGO, CA 92110-3127

SPAWARINST 3800.1D
SPAWAR 07-5
15 July 1998

SPAWAR INSTRUCTION 3800.1D

From: Commander, Space and Naval Warfare Systems Command

Subj: INTELLIGENCE SUPPORT TO SPAWAR PROGRAMS

Ref: (a) OPNAVINST 3811.1C of 16 May 1995 Threat Support to Weapons Systems Selection, Planning and Acquisition
(b) DOD Instruction 5000.2 of 23 Feb 1991, Defense Acquisition, Management, Policies, and Procedures
(c) OPNAVINST 3880.6 of 30 Aug 89, Scientific and Technical Intelligence Liaison Officer (STILO) Program and Intelligence Support for the Naval Research, Development, Test & Evaluation, and Acquisition Communities.
(d) DOD Directive S5105.21 – M1 of Mar 95 w/NAVSUP of Mar 97 (NOTAL) (U)
(e) NAVINTCOMINST 3890.1C of 12 Jul 89, Intelligence Production Tasking Procedures
(f) OPNAVINST S7030.3C of 29 Mar 83, Control Procedures for Special Interagency Support Between the Navy & Other Departments and Agencies; implementation of (U)
(g) OPNAVINST S3810.5B of 26 Dec 85, International Intelligence Agreements
(h) OPNAVINST C3490.1C of 16 Mar 82, FORMICA (U)

1. Purpose. To define policy, responsibility and procedures for ensuring that threat intelligence is acquired, considered, and used in weapons planning and development with Space and Naval Warfare Systems Command (SPAWAR), subordinate commands, and university laboratories. To designate staff elements responsible for other intelligence related programs and activities within SPAWAR. This instruction is a major revision and should be reviewed in its entirety.

2. Cancellation. SPAWARINST 3800.1C of 26 February 1992 is cancelled.

3. Background.

a. Effective 1 June 1997 the responsibility for the Intelligence, STILO, Special Security and Special Access Program support was transferred from SPAWAR 00H (SSO/STILO) to the SPAWAR Systems Center, San Diego (D017).

b. The ever increasing complexity and cost of modern naval systems make it imperative that timely, accurate scientific and technical (S&T) intelligence and other relevant threat projections be considered and applied in SPAWAR programs throughout their life cycles. Therefore, closely monitoring potential hostile forces capabilities which bear on SPAWAR system's effectiveness, is a key factor in ensuring that the fleet is supplied with truly superior warfighting equipment. Additionally, when significant changes in the threat occur, it is crucial that they be recognized early on so that modifications can be made before dollars are needlessly expended on designs which may prove inherently vulnerable or otherwise ineffective in the projected combat environment.

4. Scope. This instruction applies to all weapons, sensors and communications related programs under SPAWAR's cognizance at every planning stage from concept formulation through research, development, test and evaluation to acquisition and life cycle support. Specific subjects covered include a description of the intelligence function at SPAWAR headquarters, the Scientific and Technical Liaison Officer's (STILO) role, Sensitive Compartmented Information (SCI) management, Special Access Programs (SAP), Intelligence Related Contracting, obtaining intelligence support for SPAWAR programs, liaison with intelligence agencies and the appointment and functions of Directorate Intelligence Liaison Officers (DILOs).

5. Policy. In keeping with the policies of SECDEF, SECNAV, and CNO, SPAWAR will pursue a vigorous intelligence program, administered at the command level in support of its acquisition efforts, so that the intelligence needs of all programs are met. SPAWAR program directors and managers will ensure that a realistic assessment of system performance against expected enemy capabilities is acquired, considered, and included in program planning. References to the status of threat assessments pertinent to SPAWAR programs and their effects, if any, on threshold requirements are to be specifically included in the milestone and program review documentation.

6. Responsibility.

a. Program Managers are responsible for ensuring that adequate threat data are acquired, considered, and included in planning for systems development and acquisition or study efforts under their cognizance following the policy given in references (a) and (b), and in this instruction. They are responsible for ensuring that appropriate funding is provided for such intelligence support if required.

b. The STILO (SPAWAR Systems Center D0174) is responsible for maintaining and managing a command intelligence support function to assist program managers.

7. Management of Scientific and Technical Intelligence Support at SPAWAR.

a. Responsibility. The intelligence function at SPAWAR will be managed by the STILO, SPAWAR Systems Center D0174. The intelligence function specifically includes:

(1) Operation of SPAWAR's STILO program according to reference (c).

(2) Operation and maintenance of an intelligence library containing current information on threat systems and capabilities pertinent to SPAWAR's mission.

(3) Reviewing and advising on threat statements used in support of SPAWAR programs or study efforts.

b. Procedures.

(1) STILO Program. To improve the liaison between the Navy's technical and intelligence communities, SPAWAR operates its STILO program at the command staff level and requires subordinate commands in need of intelligence support to similarly designate STILOs. The SPAWAR STILO, SPAWAR Systems Center D0174, functions directly under the Senior Intelligence Officer. SPAWAR's STILO is charged with:

(a) Maintaining a broad overview of SPAWAR's programs and other activities for intelligence support purposes; making intelligence available to those programs and activities; and taking action to fill "intelligence gaps" where available information is not sufficient for program needs.

(b) Bringing new intelligence which might affect SPAWAR programs to the attention of the appropriate offices and key decision makers.

(c) Assisting SPAWAR program personnel in the use/interpretation of current, validated (DOD approved) threat intelligence.

(d) Coordinating the submission of requirements to the Office of Naval Intelligence and/or other intelligence agencies for intelligence data needed to support SPAWAR programs which is not available locally.

(e) Acting as primary point of contact between SPAWAR and all agencies of the Intelligence Community, coordinating visits of SPAWAR personnel to these agencies, and arranging for SPAWAR technical and engineering support to such agencies when requested.

(f) Coordinating the utilization of SPAWAR Naval Reserve Intelligence resources. This includes familiarization with all the roles specified in this document and the STILO program specific intelligence support.

(g) Facilitating the Reserve Intelligence Support provided to SPAWAR by coordinating with the PDs and PMWs to find specific intelligence support needs that would best be served through organic support. In this role the STILO program would find Reserve Intelligence personnel with aptitudes in specific areas and allow them to work directly with the technical programs supporting the acquisition process.

(2) Requesting Intelligence Support for SPAWAR programs. The STILO program, specifically SPAWAR's general service (SECRET level) intelligence library, the command's SCI facilities, the STILO's Intelligence Reservists have been established to assist program managers in obtaining the threat information required for their programs. Program personnel

requiring threat information will contact SPAWAR Systems Center D0174 to discuss their intelligence needs. All SPAWAR requests for intelligence information will be coordinated through the STILO. The STILO will adhere to the policies and procedures given in reference (e) for tasking the Intelligence Community.

(3) Liaison with Navy, other DOD, and non-DOD intelligence agencies. The STILO is the primary point of contact between the command and the U.S. Intelligence Community. In conducting business with such organizations, the following procedures apply at SPAWAR:

(a) All initial S&T liaison between SPAWAR and the U.S. Intelligence Community will be coordinated with the STILO. Direct liaison between SPAWAR personnel and specific intelligence agencies may be authorized and encouraged for long-term programs with STILO coordination. If direct liaison is authorized, SPAWAR personnel are required to keep the STILO informed on a regular basis. For purposes of this instruction, liaison is defined as electrically transmitted messages, written correspondence, telephone contact, and visits. Relevant intelligence agencies include all of the following, as well as their subordinates:

Central Intelligence Agency (CIA)
National Imagery and Mapping Agency (NIMA)
National Security Agency (NSA)
Office of Naval Intelligence (ONI)
National Maritime Intelligence Center (NMIC)
Naval Criminal Investigative Service (NCIS)
National Air Intelligence Center (NAIC)
National Ground Intelligence Center (NGIC)
Missile and Space Intelligence Center (MSIC)
All Joint Intelligence Centers (JICs)

(b) SPAWAR personnel who plan to visit any of the above commands or agencies for threat intelligence support purposes are required to inform the STILO. These procedures are not to impede contact between SPAWAR personnel and the Intelligence Community; rather, they will (1) abide by ONI guidelines to use the STILO program for access to the Intelligence Community, (2) expedite contact with the appropriate persons, (3) keep the STILO informed of command business with the Intelligence Community, (4) provide the Intelligence Community with a single point of contact for SPAWAR intelligence matters, (5) minimize inconvenience to program personnel due to possible access or entry problems at visitor control points, particularly where there are special procedural requirements, such as those at CIA, NSA, and NIMA.

(c) In addition to the requirements of paragraph 7b(3) above, reference (f) established control procedures for all contact between Navy personnel and the CIA. All SPAWAR personnel who are contacted by CIA employees wishing to visit SPAWAR will notify the Senior Intelligence Officer (D017) for assistance and visit coordination. The Senior Intelligence Officer will verify the need to visit and comply with CNO regulations to obtain the necessary authorizations. All SPAWAR personnel are cautioned that any interagency support between

SPAWAR and the CIA involving transfer of funds must be authorized by SECNAV, CNO, ONI, and the Commander. Any SPAWAR employee entering into negotiations for such interagency support with the CIA shall immediately contact the Senior Intelligence Officer. The Security Manager will not pass security clearances to the CIA without the Senior Intelligence Officer's endorsement.

(d) SPAWAR personnel who are contacted by NSA are required to contact the Senior Intelligence Officer (D017) for assistance and visit coordination. This procedure also applies in the case of any intelligence organization or detachment resident in NSA spaces.

(e) Reference (g) established procedures for contact between Navy personnel and foreign intelligence agencies. All SPAWAR personnel with a need to contact foreign agencies are required to advise the Senior Intelligence Officer before doing so where the need will be verified in order to obtain the necessary authorization.

(4) Support to Intelligence Agencies by SPAWAR personnel. To the extent that there is a scant impact on SPAWAR operations, personnel and activities under the Commander's purview are encouraged to support intelligence operations on request. The STILO has cognizance over support provided by SPAWAR to agencies of the Intelligence Community. In particular, the STILO is the command's primary point of contact for participation in the FORMICA program defined in reference (h). SPAWAR and subordinate activities routinely provide technical advice, through the STILOs to ONI in accordance with reference (h). Any request from an intelligence agency for either overt or covert support to be supplied by SPAWAR employees shall be immediately reported as follows:

(a) If the requested support does not involve technical services and/or is not related to the commands sponsored projects (as is generally the case with FORMICA activities), the STILO shall be informed of the request.

(b) If the requested support is S&T in nature and related to ongoing or planned SPAWAR technical projects but purely advisory, the STILO and the cognizant program directors and managers shall be made aware of the request.

(c) All requests for the physical involvement of SPAWAR employees in clandestine or covert intelligence operations or in any operation which entails expending SPAWAR funds, significant manpower or other resources must be brought to the attention of the Commander, SPAWAR. There will be no SPAWAR participation in such operations without prior knowledge and approval of the Commander.

(5) Technical Support to NMIC

(a) NMIC is the primary producer of Navy S&T threat data, and therefore, supplies directly and indirectly much of the intelligence supplied at SPAWAR RDT&E efforts. A special relationship between the NMIC and SPAWAR is properly characterized by a high degree of mutual support.

(b) NMIC is unable, for a variety of reasons, to employ sufficient numbers of resident technologists to address the many diverse disciplines of interest to the systems acquisition community. SPAWAR and subordinates have "in house" expertise covering a broad range of S&T endeavors. This reservoir of capability should be used when practicable to provide consulting or engineering support for NMIC to fully exploit available S&T information. This expertise can also provide authoritative guidance on future developments and directions of key technologies, especially where it is clear that the pay-off of an exploitation project will have a bearing on SPAWAR programs.

8. Sensitive Compartmented Information (SCI) Program. The SCI program at SPAWAR is administered by the Special Security Officer (SSO), D017, who functions directly under the Senior Intelligence Officer, and the Special Security Office, D0171 at SPAWAR Systems Center San Diego. The duties and responsibilities of the SSO are defined in reference (d). The SSO:

a. Maintains custody, physical security, and access control of all SCI facilities and locally held materials, to include SCI security oversight.

b. Manages all SCI employee billets assigned to Command. Validates need-to-know and priority in assigning SCI billets. Contractor billet management see SAP program.

c. Acts as the security point of contact for the Command's sensitive compartmented information (SCI) program.

d. Coordinates and provides assistance to program managers and sensitive compartmented information facility (SCIF) managers in the preparation and creation of standard operating procedures for SCIFs and SCI programs within SCIFs as required by reference (d).

e. Maintains accurate records of all Command personnel with SCI access; transmits all SCI clearances for Command personnel; receives and verifies SCI access status of all visitors who require access to Command SCIFs and is the certification officer for all SCI access.

f. Provides classification and marking guidance for SCI generated material generated in the Command.

g. Maintains the SCI Station Profile (budget), ensuring unique SCI functions, equipment requirements, training and travel are adequately planned for and funded.

h. Maintains applicable SCI directives, regulations, manuals and guidelines to adequately discharge SSO duties and responsibilities.

i. Ensures all SCI is properly accounted for, controlled, transmitted, transported, packaged and safeguarded. Ensures all SCI material is destroyed in authorized destruction facilities and in accordance with reference (d).

j. Ensures SCI is disseminated only to persons authorized access to the material and having an established need-to-know.

k. Provides guidance and assistance for processing SCI position and eligibility requests.

l. Conducts SCI security briefings, indoctrinations, and debriefings; obtains signed Nondisclosure Agreements; and performs other related personnel security actions.

m. Investigates SCI security infractions, making recommendations and preparing reports.

n. Interfaces with the ISSO/ISSM/AIS and physical security representatives ensuring SCI continuity with SSO functions and requirements.

o. Conducts a continuing SCI security education and awareness program to ensure that all SCI indoctrinated individuals are kept apprised of requirements and guidelines for protecting SCI.

p. Reviews all derogatory information from the local supporting military law enforcement agency involving SCI-indoctrinated personnel and takes appropriate action.

q. Maintains continuing liaison with SCI and non-SCI security officials.

r. Provides Statement of Personal History and associated forms to initiate Single Scope Background Investigation (SSBI) and furnish guidance for their completion to all Command personnel needing access to SCI material. Submits investigative forms to appropriate agencies.

s. Acts as point of contact, coordinating and providing SCI security guidance to SCI conferences and symposia held at the Command.

9. Special Access Programs. The Special Access Programs (SAP) are administered by the Program Support Office, D0173 of SPAWAR Systems Center San Diego, which functions directly under the Senior Intelligence Officer. The Program Support Office:

a. Maintains custody, physical security and access control of all SAP facilities and locally held materials.

b. Assists in the Office of Naval Intelligence approval of all contracts requiring contractor access to SCI. Acts as the supporting Security Office for all SCI and SAP contracts.

c. Manages all contractor SCI billets assigned to SPAWAR. Need-to-know and priority in assigning the contractor SCI billets will be the combined responsibility of the Program Support Office and Contracting Officer Representative (COR).

d. Acts as the security point of contact for the command for all compartmented SAP programs.

e. Coordinates and provides assistance to program managers in creation of Program Protection Plans and Systems Security Engineering Management Programs in the area of compartmented programs as required by reference (d).

f. Certifies, in coordination with program directors and managers, need-to-know for contractor personnel working on SPAWAR contracts requiring access to SCI materials.

g. Provides classification guidance material with respect to SAP programs.

10. Directorate Intelligence Liaison Officers (DILOS). In support of the command's Intelligence Program, each program directorate may choose to designate a management level representative and an alternate to act as DILO. Primarily, DILOs function as technically knowledgeable points of contact in the relationship between the directorate and the Intelligence Program. In that capacity, DILOs are expected to:

a. Assist in expediting and coordinating their directorates transactions with the STILO office. Such transactions include annual review and update of applicable Systems Threat Assessment Reports (STARs) and Critical Intelligence Parameters (CIPs) as required by reference (b). DILOs are responsible for keeping the STILO informed of developments of new projects in their directorates that may alter existing or generate new intelligence data requirements.

b. Be active participants in the Intelligence Program to the extent of keeping up on S&T intelligence matters by attending STILO briefs and reading relevant documentation identified by the STILO. They are specifically tasked with assisting the STILO, on an "as required" basis, in contacting appropriate directorate personnel to ensure they are made aware of intelligence information affecting their respective programs.

11. Action. Effective immediately SPAWAR Headquarters and SPAWAR System Centers shall utilize the guidance and shall comply with the policies and procedures set forth in this instruction.

ROBERT J. MARTIN
Deputy Commander

Distribution:
SPAWAR List 3

SNDL Part 2
FKQ (SPAWAR Systems Centers)